

Девятая конференция «Информационная безопасность АСУ ТП КВО»

17–18 марта 2021 г.

г. Москва

ПРОГРАММА

День первый

09.00–10.15

Регистрация. Работа выставки

10.15–13.30

Пленарное заседание

- Вступительное слово ведущего – *Гаврилов Виктор Евдокимович, главный научный сотрудник, Федеральный исследовательский центр Информатика и управление Российской академии наук*
- Вопросы реализации законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации – *Торбенко Елена Борисовна, заместитель начальника Управления ФСТЭК России*
- Правовое регулирование информационной безопасности в Республике Беларусь – *Вяткин Денис Николаевич, начальник отдела Оперативно-аналитического центра при Президенте Республики Беларусь*
- А взломы здесь тихие: контроль пользователей с привилегиями – *Бочкарёв Сергей Вячеславович, директор по развитию бизнеса «АйТи Бастион»*
- Выявление и ликвидация последствий компьютерных инцидентов в АСУ ТП – *Алексей Шанин, директор компании «СайберЛимфа»*
- Как защитить АСУ ТП от кибератак, обеспечить непрерывность промышленных процессов и выполнить 187-ФЗ: на примере системы InfoWatch ARMA – *Игорь Душа, технический директор InfoWatch ARMA*
- Конфиденциальность – отсутствующий элемент современной ИТ-инфраструктуры – *Петросюк Георгий Георгиевич, директор департамента информационных технологий НИЦ «Институт имени Н.Е. Жуковского»*

13.30–14.30

Обеденный перерыв. Работа выставки

129626, Москва, ул. 3-я Мытищинская, д. 3, стр. 1

(495) 925-11-18

www.connect.ru

Требования регулятора, угрозы и риски, методики и методы защиты АСУ ТП

- Тренды, уязвимости и защита технологических сетей КВО РФ – *Анастасьев Алексей Владимирович, руководитель направления по развитию бизнеса Positive Technologies*
- Мониторинг АСУТП. Практические аспекты – *Прошин Андрей Владимирович, руководитель направления по развитию бизнеса услуг и сервисов SOC «Ростелеком-Солар»*
- Мониторинг информационной безопасности в АСУ ТП на ядре из СОВ: от базовых требований к лучшим практикам – *Шайхутдинов Азат Ильясович, менеджер по развитию бизнеса Kaspersky ICS*
- Центр обеспечения безопасности: как не утонуть в потоке событий ИБ? – *Николай Домуховский, заместитель генерального директора по научно-технической работе УЦСБ*
- Совместное решение Dr.Web и DATAPK для защиты объектов КИИ – *Василий Севостьянов, начальник отдела технического сопровождения продаж ООО «Доктор Веб»*
- Устройства класса диод как средство защиты периметра сети: мифы и реальность – *Половинко Вячеслав Владимирович, руководитель направления собственных продуктов, Департамент информационных систем АМТ-ГРУП*
- Реализация системы обеспечения кибербезопасности электроэнергетической компании – *Мареев Денис Игоревич, начальник Департамента информационной безопасности, АО «ОЭК»*
- Практические аспекты создания системы обеспечения информационной безопасности АСТУ электросетевой компании – *Сердюк Виктор Александрович, генеральный директор АО «ДиалогНаука»*
- Практика импортозамещения в КИИ. Российский индустриальный межсетевой экран/ криптошлюз/ маршрутизатор – *нужное подчеркнуть – Сорокина Марина Викторовна, руководитель направления, отдел развития продуктов АО «ИнфоТеКС»*

- Автоматизация процессов соответствия требованиям 187-ФЗ – *Носова Ирина Евгеньевна, ведущий пресейл-менеджер R-Vision*
- Компьютерные атаки, направленные на нарушение штатного функционирования систем железнодорожной автоматики – *Безродный Борис Федорович, доктор технических наук, профессор, заместитель руководителя Центра кибербезопасности АО «НИИАС»*
- О страховании информационных рисков АСУ ТП – *Воеводин Владислав Александрович, доцент кафедры «Информационная безопасность» Московский институт электронной техники*

18.45–20.00

Фуршет

День второй

09.00–10.00

Регистрация участников. Работа выставки

10.00–11.30

Дискуссионная панель по вопросам импортозамещения в сфере ИБ АСУ ТП

Модератор

Петросюк Георгий Георгиевич, директор департамента информационных технологий НИЦ «Институт имени Н.Е. Жуковского»

Участники

Афонин Владимир Николаевич, начальник отдела информационной безопасности АО «Корпорация «МИТ»

Домуховский Николай, заместитель генерального директора по научно-технической работе «УЦСБ»

Душа Игорь, технический директор «ИНФОВОТЧ АРМА»

Нуйкин Андрей Витальевич, начальник отдела «ЕВРАЗ»

Осмехин Александр Николаевич, инженер по ИТ АО «ОКБМ Африкантов»

Родин Константин Сергеевич, руководитель технического центра ООО «АйТи БАСТИОН»

Трушкин Константин Александрович, заместитель директора по маркетингу АО "МЦСТ"

Щербаков Михаил Александрович, Заместитель начальника отдела ПД ИТР и ТЗИ, АО "ВОТКИНСКИЙ ЗАВОД"

Вопросы

- Импортозамещение и информационная безопасность. Как соотносится импортозамещение и обеспечение защиты критических информационных систем? Можно ли гарантированно обеспечить безопасность иностранного ПО? Стоит ли использовать иностранные ИБ-решения, если российские не имеют необходимого функционала? Все ли продукты, отечественное происхождение которых доказано, действительно являются безопасными?

- **Импортозамещение и функционал.** Есть ли отставание в развитии технологий между российскими и иностранными средствами защиты? Какие российские технологии защиты находятся на международном уровне и где функционал недостаточен? Насколько функционал самих российских АСУ ТП отстает от иностранных аналогов в части обеспечения информационной безопасности?
- **Отечественное и свободное.** Какая часть российских средств защиты базируется на ПО с открытыми исходным кодом? Насколько российские разработчики могут влиять на разработку ПО с открытыми исходным кодом? Как в свободном ПО обстоит дело с проверкой безопасности исходных кодов?
- **Особенности импортозамещения ИБ в АСУ ТП.** Насколько российские решения АСУ ТП отвечают требованиям по информационной безопасности? Часто ли в проектах по импортозамещению АСУ ТП возникают требования по ИБ? Многие ли российские производители средств АСУ ТП внедрили стандарты безопасной разработки?
- **Обновления и вредоносные обновления.** Насколько в России реализуема атака через обновления ПО, которая была организована через компании M.E.Doc и SolarWinds? Как организовать проверку обновлений и защиту от атак через обновления для промышленных информационных систем (АСУ ТП, SCADA, MES)? Кто должен делать дополнительные проверки обновлений для конкретного оборудования и конфигурации?

11.30–13.30

Отраслевой опыт. Практика эксплуатации и защиты АСУ ТП.

- **Импортонезависимые решения на базе российской аппаратной платформы –** *Минаков Артем Евгеньевич, начальник отдела информационной безопасности ЗАО «НОРСИ-ТРАНС»*
- **Процессы обеспечения ИБ АСУ ТП ПАО «Транснефть» и организаций системы «Транснефть» –** *Кобзев Дмитрий Александрович, заместитель начальника отдела ИБ АСУ ТП ПАО «Транснефть»*
- **Новый подход по классификации объектов КИИ –** *Губайдуллин Артем Рифович, заместитель руководителя по реализации проектов в области Индустрия 4.0, ОАО «ММК-МЕТИЗ»*

- Обеспечение безопасности объектов критической информационной инфраструктуры. Опыт ПАО «НЛМК» – *Овчинников Алексей Геннадьевич, начальник Управления информационной безопасности ПАО «НЛМК»*
- Реализация проекта по созданию корпоративного SOC для отслеживания угроз безопасности и предотвращения атаки на инфраструктуру всех ключевых предприятий и информационных систем ТМК – *Кокин Антон Александрович, начальник Управления средств защиты ИТ-инфраструктуры ПАО «ТМК»*
- Опыт создания корпоративного сегмента ГосСОПКА для Госкорпорации «Роскосмос» – *Графеев Олег Евгеньевич, начальник отдела мониторинга информационной безопасности ФГУП «НТЦ «Заря»*
- Мы знаем, что вы делали прошлым летом. Повышаем качество аналитики в системах контроля пользователей – *Родин Константин Сергеевич, руководитель технического центра «АйТи Бастион»*

13.30–14.30

Обеденный перерыв. Работа выставки

14.30–17.45

**Отраслевой опыт. Практика эксплуатации и защиты АСУ ТП
(продолжение). Подготовка кадров**

- Методическое обеспечение процессов категорирования объектов КИИ ОАО «РЖД» – *Хмелевская Наталья Владимировна, заместитель начальника отдела мониторинга и анализа угроз безопасности, Центр компетенций по информационной безопасности – структурное подразделение ОАО «РЖД»*
- Анализ безопасности энергоблока АЭС, обусловленный воздействием компьютерных атак на АСУ ТП АЭС. Подход и основные аспекты – *Бабаев Денис Игоревич, начальник отдела нормативно-технического обеспечения кибербезопасности, АО «ВНИИАЭС»*
- Анализ трафика ip-сетей в сегментах АСУТП: выявление аномалий – *Горлянский Дмитрий Александрович, руководитель технического сопровождения клиентов Гарда Технологии*

- Как применять аналитические средства для обеспечения безопасности АСУ ТП предприятий ТЭК – *Большаков Анатолий Афанасьевич, начальник отдела службы технического директора «Газинформсервис»*
- Защита в рамках цифровизации промышленных предприятий (АСУТП) – *Гаращенко Дмитрий Владимирович, начальник отдела информационной безопасности, АО «НПП «Исток» Им. Шокина»*
- Новые образовательные и профессиональные стандарты для кадрового обеспечения информационной безопасности Российской Федерации – *Белов Евгений Борисович, заместитель председателя Федерального учебно-методического объединения в системе высшего образования по УГСНП 10.00.00 «Информационная безопасность, председатель ФУМО СПО ИБ*
- Особенности формирования образовательных программ в соответствии с требованиями новых образовательных стандартов по направлению "Информационная безопасность" – *Хорев Анатолий Анатольевич, заведующий кафедрой ИБ, НИУ МИЭТ*

17.45–18.00

Подведение итогов конференции